Patrice L. Bishop (182256)
pbishop@ssbla.com
STULL, STULL & BRODY
9430 W. Olympic Blvd., Suite 400
Beverly Hills, CA 90212
Tel: 310-209-2468
Fax: 310-209-2087

Counsel for Plaintiff

(Additional Counsel on Signature Page)

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

BRITTANY DURGIN, Individually and on Behalf of all Others Similarly Situated, Plaintiff, v. RASIER, LLC, RASIER-CA, LLC, and UBER TECHNOLOGIES, INC., Defendants.	Case No. 3:18-cv-01785 **COMPLAINT** **CLASS ACTION** **DEMAND FOR JURY TRIAL**

Plaintiff Brittany Durgin ("Plaintiff"), by and through her undersigned counsel, submits this Complaint on behalf of herself and all others similarly situated. Plaintiff's allegations are based upon her personal knowledge as to herself and her own acts, and upon information and belief, developed from the investigation and analysis by Plaintiff's counsel, including a review of publicly available information.

NATURE OF THE ACTION

1. Plaintiff brings this class action case against Rasier, LLC., Rasier-CA, LLC., Uber Technologies, Inc. (collectively referred to as either "Uber" or "Defendants") for their failure to secure and safeguard riders' and drivers' personally identifiable information ("PII") which Uber collected in connection with the operation of its business.

2. On November 21, 2017, Uber disclosed that in October 2016 hackers had stolen 57 million driver and rider accounts (the "Data Breach" or "Breach") and that Defendants had kept the data breach secret for more than a year after paying a $100,000 ransom.

3. Uber has acknowledged that a cybersecurity incident occurred, resulting in the theft of its riders' and drivers' PII, consisting of names, addresses, email addresses, credit card numbers and other information.

4. The PII of Plaintiff and the class of riders she seeks to represent was compromised due to Uber's acts and omissions and their failure to properly protect their PII.

5. Uber could have prevented this Data Breach.

6. Uber disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to disclose to its riders the material fact that it did not have adequate security practices to safeguard PII, failing to take available steps to prevent and stop the breach from ever happening, and failing to monitor and detect the breach on a timely basis.

7. As a result of the Data Breach, Plaintiff's and Class members' PII has been exposed, in all likelihood, to criminals for misuse. The injuries suffered by Plaintiff and Class members, or likely to be suffered as a direct result of the Data Breach, include:

a. unauthorized use of their PII;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PII;

e. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit, including decreased credit scores and adverse credit notations;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, the costs of purchasing credit monitoring and identity theft protection services, and the stress, nuisance and annoyance of dealing with all issues arising from the Data Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII being placed in the hands of criminals and already misused via the sale of Plaintiff and Class members' information on the Internet black market;

h. damages to and diminution in value of their PII entrusted to Uber for the sole purpose of purchasing services from Uber; and

i. the loss of Plaintiff's and Class members' privacy.

8. The injuries to the Plaintiff and Class members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for PII.

9. Further, Plaintiff retains a significant interest in ensuring that her PII, which, while stolen, remains in the possession of Defendants, is protected from further breaches, and seeks to remedy the harms she has suffered on behalf of herself and similarly situated riders and drivers whose PII was stolen as a result of the Data Breach.

10. Plaintiff brings this action to remedy these harms on behalf of herself and all similarly situated individuals whose PII was accessed during the Data Breach. Plaintiff seeks the

following remedies, among others: actual and/or statutory damages, and multiple damages, under state and/or federal laws, reimbursement of out-of-pocket losses, other compensatory damages, further and more robust credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Defendants to implement improved data security measures.

PARTIES

11. Plaintiff is a Massachusetts citizen, and was an Uber rider in October 2016.

12. Defendant Rasier, LLC is a Limited Liability Company with its headquarters and principal place of business in San Francisco, California.

13. Defendant Rasier-CA, LLC is a Limited Liability Company with its headquarters and principal place of business in San Francisco, California.

14. Defendant Uber Technologies, Inc. is a corporation with its headquarters and principal place of business and corporate offices in San Francisco, California and is the parent company of Defendants Rasier and Rasier-CA.

15. Defendants develop, market, and operate a ridesharing mobile application which allows consumers to submit a trip request, which is routed to crowd-sourced taxi drivers. Their smartphone application connects drivers with people who need a ride. Uber's application enables users to arrange and schedule transportation and/or logistics services with third party providers.

JURISDICTION AND VENUE

16. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d)(2), because the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and Plaintiff and Defendants are citizens of different states. The proposed Class and Sub-class each include well over 100 members.

17. This Court has jurisdiction over Defendants because Defendants are located within this District, regularly conduct business in California; and have sufficient minimum contacts in California. Defendants intentionally avail themselves of this jurisdiction by marketing and offering their services from California to millions of consumers nationwide, including Uber riders in the Commonwealth of Massachusetts.

18. Venue is proper in this District pursuant to 28 U.S.C. §1391 because Defendants are located within this District.

CLASS ACTION ALLEGATIONS

19. Plaintiff brings this class action pursuant to Federal Rules of Civil Procedure 23(a) and (b)(3), on behalf of herself and all others similarly situated in the United States, who were Uber riders during and since the Data Breach, had their personal information stolen from Uber's software application systems, and were damaged thereby (the "Class"). Plaintiff also brings Count I on behalf of a Sub-class of Massachusetts residents who were Uber riders during and since the Data Breach and had their personal information stolen from Uber's software application systems and were damaged thereby (the "Massachusetts Sub-class" or "Sub-class"). The Class and Sub-class do not include Uber officers or directors.

20. The Class and Massachusetts Sub-class consist of potentially millions of Uber riders. While the exact number of Class and Sub-class members and the identities of individual Class and Sub-class members are unknown to Plaintiff's counsel at this time, and can only be ascertained through appropriate discovery, based on the fact that 57 million Uber riders and drivers have been adversely affected, the membership of the Class and Sub-class are each so numerous that joinder of all members is impracticable.

21. Uber's wrongful conduct affected all members of the Class and Sub-class in exactly the same way. Defendants' failure to properly safeguard its customer's personal information is completely uniform among the Class and Sub-class.

22. Questions of law and fact common to all members of the Class and Sub-class predominate over any questions affecting only individual members. Such common questions of law and fact include:

a. whether Defendants acted wrongfully by failing to properly safeguard their riders' personal information collected and stored by Uber on its software application system;

b. whether Defendants' conduct violated the law;

c. whether Plaintiff and the other members of the Class and Sub-class have been damaged, and, if so, what is the appropriate relief; and

d. whether Defendants breached their duties owed to members of the Class and Sub-class by failing to properly safeguard their personal information.

23. Plaintiff's claims, as described herein, are typical of the claims of all other members of the Class and Sub-class, as the claims of Plaintiff and all other members of the Class and Sub-class arise from the same set of facts regarding Defendants' failure to protect the Class and Sub-class members' PII from computer hackers. Plaintiff maintains no interest antagonistic to the interests of other members of the Class or Sub-class.

24. Plaintiff is committed to the vigorous prosecution of this action and has retained competent counsel experienced in the prosecution of class actions of this type. Accordingly, Plaintiff is an adequate representative of the Class and Sub-class and will fairly and adequately protect their interests.

25. This class action is a fair and efficient method of adjudicating the claims of Plaintiff and the Class and Sub-class for the following reasons:

a. common questions of law and fact predominate over any question affecting any individual Class and Sub-class members;

b. the prosecution of separate actions by individual Class and Sub-class members would likely create a risk of inconsistent or varying adjudications with respect to individual members thereby establishing incompatible standards of conduct for Defendants or would allow some Class and Sub-class members' claims to adversely affect the ability of other members to protect their interests;

c. this forum is appropriate for litigation of this action since a substantial portion of the transactions, acts, events, and omissions alleged herein occurred in this District;

d. Plaintiff anticipates no difficulty in the management of this litigation as a class action; and

e. the Class and Sub-class are readily definable, and prosecution as a class action will eliminate the possibility of repetitious litigation, while also providing redress for

claims that may be too small to support the expense of individual, complex litigation.

26. For these reasons, a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

SUBSTANTIVE ALLEGATIONS

27. Plaintiff was a rider with Uber prior to and during October 2016 and to the present, and provided PII to Uber in order to initiate her Uber account to be used solely by Uber for purposes of maintaining and facilitating such account.

28. On November 21, 2017, Uber announced that two hackers had stolen data about Uber's riders and drivers from a third-party server and then approached Uber and demanded payment of $100,000 to delete their copy of the data. Defendants discovered this breach as part of a larger investigation into Uber's business practices over a year ago.

29. Joe Sullivan, the Uber chief security officer at the time of the breach, who has since been fired, arranged the deal to pay the hackers the $100,000 in ransom. However, Uber did not stop at acquiescing to the hacker's demands and took it a step further. Uber successfully tracked down the hackers and forced them to sign nondisclosure agreements.

30. To further conceal the damage caused from this breach, Uber executives made it appear that rather than this payment being a ransom payoff, they made the payoff appear to be part of a "bug bounty" which is a deal offered by many websites and software developers whereby individuals can receive recognition and compensation for reporting "bugs," especially those pertaining to exploits and vulnerabilities in a company.

31. The failure to immediately or within a reasonable time report this data breach to relevant governmental agencies and to Uber users and drivers is a blatant and egregious violation of numerous state statutes specifically enacted to insure prompt disclosure of data breaches.

32. For example, Uber's failure to directly notify its riders affected by the Data Breach (including Plaintiff and Sub-class members), and to notify the appropriate regulatory authorities, violated the provisions of M.G.L., c. 93H, and in particular the reporting provisions of c. 93H, § 3, which required Uber, once it knew or had reason to know of a data security breach involving

personal information and affecting Massachusetts residents, to provide prompt and direct notice of such breach to any affected Massachusetts residents, to the Massachusetts attorney general, and to the director of consumer affairs and business regulation for Massachusetts.

33. Plaintiff and Class members have suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by their PII being placed in the hands of criminals who have already, or will imminently, misuse such information.

34. Moreover, Plaintiff has a continuing interest in ensuring that her PII, which remains in the possession of Uber, is protected and safeguarded from future breaches.

35. At all relevant times, Uber was well-aware, or reasonably should have been aware, that the PII collected, maintained and stored by Uber is highly sensitive, susceptible to attack, and could be used for wrongful purposes, such as identity theft and fraud.

36. It is well known and the subject of many media reports that PII is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches, Uber continued to use an outdated, insufficient and inadequate system to protect the PII of Plaintiff and Class members.

37. PII is a valuable commodity because it contains not only payment card numbers but other PII as well. A "cyber blackmarket" exists in which criminals openly post stolen payment card numbers and other personal information on a number of underground Internet websites. It is common knowledge that PII is considered gold to identity thieves because they can use victims' personal data to incur charges on existing accounts, or clone ATM, debit, or credit cards.

38. Legitimate organizations and the criminal underground alike recognize the value in PII contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data [containing PII] from 38 million users."[1]

[1] Verizon 2014 PCI Compliance Report, available at: http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (hereafter "2014 Verizon Report"), at 54 (last visited March 16, 2018).

39. At all relevant times, Uber knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on individuals as a result of a breach.

40. Uber was, or should have been, fully aware of the significant number of people whose PII it collected, and thus, the significant number of individuals who would be harmed by a breach of its system.

41. Unfortunately, and as alleged below, despite all of this publicly available knowledge of the continued compromises of PII in the hands of other third parties, Uber's approach to maintaining the privacy and security of the PII of Plaintiff and the Class members, and reporting any violation thereof in accordance with law, was lackadaisical, cavalier, reckless, or at the very least, negligent.

42. The ramifications of Uber's failure to keep Plaintiff's and Class members' data secure are severe.

43. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[2] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[3]

44. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[4]

[2] 17 C.F.R § 248.201 (2013).

[3] *Id.*

[4] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited March 16, 2018).

45. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[5]

46. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[6]

47. There may be a time lag between when harm occurs and when it is discovered, and also between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[7]

48. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

49. The PII of Plaintiff and the Class members is private and sensitive in nature and was left inadequately protected by Uber.

50. The Data Breach was a direct and proximate result of Uber's failure to properly safeguard and protect Plaintiff's and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the

---

[5] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited March 16, 2018).

[6] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited March 16, 2018).

[7] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited March 16, 2018).

common law, including Uber's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and the Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

51. Uber had the resources to prevent a breach, but neglected to timely and adequately invest in data security, despite the growing number of well-publicized data breaches.

52. Had Uber remedied the deficiencies in its data security systems, followed security guidelines, and adopted security measures recommended by experts in the field, Uber would have prevented the Data Breach and, ultimately, the theft of its customers' PII.

53. As a direct and proximate result of Uber's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives.

54. While the PII of Plaintiff and members of the Class has been stolen, Uber continues to hold PII of consumers, including Plaintiff and the Class members. Particularly because Uber has demonstrated an inability to prevent a breach and immediately disclose it even after being detected, Plaintiff and Class members have an undeniable interest in insuring that their PII is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

COUNT I

NEGLIGENCE

(ON BEHALF OF PLAINTIFF AND THE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE SUB-CLASS)

55. Plaintiff incorporates and re-alleges all allegations contained in the preceding paragraphs as if fully set forth herein.

56. Upon accepting and storing the PII of Plaintiff and Class Members in their computer systems and on their networks, Defendants undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care to secure and safeguard that information and to use

commercially reasonable methods to do so. Defendants knew that PII was private and confidential and should be protected as private and confidential.

57. Defendants owed a duty of care not to subject Plaintiff, along with her PII, and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

58. Defendants owed numerous duties to Plaintiff and to members of the Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII in its possession;

b. to protect PII using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

59. Defendants also breached their duty to Plaintiff and Class Members to adequately protect and safeguard PII by knowingly disregarding standard information security principles, despite obvious risks. Further, Defendants failed to provide adequate supervision and oversight of the PII with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Plaintiff's and Class members' PII, misuse that PII and intentionally disclose it to others without consent.

60. Defendants knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security. Defendants knew about numerous well-publicized data breaches, in addition to their own previous data breach (in 2014).

61. Defendants knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiff's and Class Members' PII.

62. Defendants breached their duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiff and Class Members.

63. Because Defendants knew that a breach of their systems would damage millions of individuals, including Plaintiff and Class members, Defendants had a duty to adequately protect their data systems and the PII contained thereon.

64. Defendants' own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their PII. Defendants' misconduct included failing to: (1) secure its systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

65. Defendants also had independent duties under state and/or federal laws that required it to safeguard Plaintiff's and Class members' PII.

66. Defendants breached their duties to Plaintiff and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PII;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiff's and Class members' PII both before and after learning of the Data Breach; and

d. by failing to comply with the minimum industry data security standards during the period of the Data Breach.

67. Through Defendants' acts and omissions described in this Complaint, including Defendants' failure to provide adequate security and their failure to protect Plaintiff's and Class members' PII from being foreseeably captured, accessed, disseminated, stolen and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' PII during the time it was within their possession or control.

68. Upon information and belief, Uber improperly and inadequately safeguarded Plaintiff's and Class members' PII in deviation from standard industry rules, regulations, and

practices at the time of the unauthorized access. Defendants' failure to take proper security measures to protect sensitive PII of Plaintiff and Class members, as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiff's and Class member' PII.

69. Defendants' conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class members' PII; and failing to provide Plaintiff and Class members with timely and sufficient notice that their sensitive PII had been compromised.

70. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

71. As a direct and proximate result of the Defendant's conduct, Plaintiff and the other members of the Class and Sub-class suffered damages including, but not limited to, loss of control of their PII, the burden and cost of heightened monitoring for signs for identity theft, and having to undertake actions such as credit freezes and alerts to prevent identity theft, and remediating acts and damages caused by identity theft, and other economic damages.

COUNT II

NEGLIGENCE *PER SE*

(ON BEHALF OF PLAINTIFF AND THE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE SUB-CLASS)

72. Plaintiff incorporates and re-alleges all allegations contained in the preceding paragraphs as if fully set forth herein.

73. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Uber, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

74. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein.

75. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

76. Plaintiff and the Class Members are within the class of persons that the FTC Act was intended to protect.

77. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

78. As a direct and proximate result of Defendant's conduct, Plaintiff and the other members of the Class and Sub-class suffered damages including, but not limited to, loss of control of their PII, the burden and cost of heightened monitoring for signs for identity theft and for having to undertake actions such as credit freezes and alerts to prevent identity theft, and remediating acts and damages caused by identity theft, and other economic damages.

COUNT III

BREACH OF IMPLIED CONTRACT

(ON BEHALF OF PLAINTIFF AND THE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE SUB-CLASS)

79. Plaintiff incorporates and re-alleges the allegations contained in the preceding paragraphs as if fully set forth herein.

80. By providing Plaintiff's and the other Class and Subclass members' PII to Uber, Plaintiff and the other members of the Class and Sub-class entered into implied contracts with Uber pursuant to which Uber agreed to safeguard and protect such information from unauthorized access and theft.

81. Plaintiff and the other members of the Class and Sub-class fully performed their obligations under the implied contracts with Uber.

82. Defendants breached the implied contracts they had made with Plaintiff and the other members of the Class and Sub-class by failing to safeguard and protect the personal and financial information of Plaintiff and the other members of the Class and Sub-class, and by

allowing unauthorized access to Uber's software application network and the mass exporting of PII from Uber.

83. The damages to Plaintiff and the other members of the Class and Sub-class as described herein were the direct and proximate result of the Defendants' breaches of these implied contracts.

COUNT IV

DECLARATORY JUDGMENT

(ON BEHALF OF PLAINTIFF AND THE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE SUB-CLASS)

84. Plaintiff incorporates and re-alleges all allegations contained in the preceding paragraphs as if fully set forth herein.

85. As previously alleged, Plaintiff and Class members entered into an implied contract that required Uber to provide adequate security for the PII it collected from their payment card transactions. As previously alleged, Uber owes duties of care to Plaintiff and Class members that require it to adequately secure PII.

86. Uber still possesses PII pertaining to Plaintiff and Class members.

87. Uber has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems.

88. Accordingly, Uber has not satisfied its contractual obligations and legal duties to Plaintiff and Class members. In fact, now that Uber's lax approach towards data security has become public, the PII in its possession is more vulnerable than it previously was.

89. Actual harm has arisen in the wake of the Uber Data Breach regarding Uber's contractual obligations and duties of care to provide data security measures to Plaintiff and Class members.

90. Plaintiff, therefore, seek a declaration that (a) Uber's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Uber must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Uber's systems on a periodic basis, and ordering Uber to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting PII by, among other things, creating firewalls and access controls so that if one area of Uber is compromised, hackers cannot gain access to other portions of Uber systems;

e. purging, deleting, and destroying in a reasonably secure manner PII not necessary for its provision of services;

f. conducting regular database scanning and security checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Uber customers must take to protect themselves.

COUNT V

VIOLATION OF THE MASSACHUSETTS CONSUMER PROTECTION ACT, M.G.L., C. 93A, § 2, BROUGHT UNDER M.G.L., C. 93A, § 9

(ON BEHALF OF PLAINTIFF THE MASSACHUSETTS SUB-CLASS)

91. Plaintiff incorporates and re-alleges all allegations contained in the preceding paragraphs as if fully set forth herein.

92. M.G.L., c. 93A, § 2 provides that "[u]nfair methods of competition and unfair or deceptive acts and practices in the conduct of any trade or commerce are declared unlawful."

93. M.G.L., c. 93A, § 9 permits any consumer injured by a violation of c. 93A, § 2 to bring a civil action, including a class action, for damages and injunctive relief.

94. At all relevant times, Uber engaged in trade or commerce in Massachusetts.

95. Plaintiff and Massachusetts Sub-class members entrusted Uber with their PII.

96. As alleged herein this Complaint, Uber engaged in unfair competition and unfair and deceptive acts or practices in trade or commerce, including the following, in violation of the c. 93A, § 2:

a. failure to maintain the security of Plaintiff's and Massachusetts Subclass Members' PII;

b. failure to maintain adequate data security practices to safeguard Plaintiffs' and Massachusetts Subclass members' PII;

c. failure to disclose that its data security practices were inadequate to safeguard Plaintiff's PII from theft; and

d. continued acceptance of PII and storage of other personal information after Uber knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach;

97. Uber knew or should have known that its data security practices were inadequate to safeguard the PII of Plaintiff and the Massachusetts Subclass members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

98. Uber's conduct in violation of M.G.L., c. 93A, § 2 was willful and knowing, within the meaning of c. 93A, § 9(3).

99. As a direct and proximate result of Uber's violation of c. 93A, § 2, Plaintiff and Massachusetts Subclass members suffered damages arising from the breach of their PII. The full nature and extent of the damages and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

100. As a direct result of Uber's knowing violation of c. 93A, § 2, Plaintiff and Massachusetts Subclass members are entitled to damages as well as injunctive relief, including, but not limited to:

a. Ordering that Uber engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Uber's systems on a periodic basis, and ordering Uber to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Uber engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Uber audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Uber segment PII by, among other things, creating firewalls and access controls so that if one area of Uber is compromised, hackers cannot gain access to other portions of Uber systems;

e. Ordering that Uber purge, delete, and destroy in a reasonable secure manner PII not necessary for its provisions of services;

f. Ordering that Uber conduct regular database scanning and securing checks;

g. Ordering that Uber routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Uber to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Uber customers must take to protect themselves.

101. Plaintiff and the Massachusetts Sub-class seek actual damages or statutory damages, whichever results in a greater recovery, and multiple damages and injunctive relief, plus attorney's fees and costs, pursuant to Federal Rule of Civil Procedure 23 and M.G.L., c. 93A, §§ 9(3) and (4), to be proven at trial.

102. Plaintiff made a written demand for relief upon Uber, on February 12, 2018, pursuant to M.G.L., c. 93A, § 9(3).

103. Uber has failed to make a reasonable offer of relief in response to the demand.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, respectfully requests that this Court:

A. Certify this action as a class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3), and appoint the Plaintiff as Class and Sub-class representatives and her counsel as Class counsel;

B. Award Plaintiff and the other members of the Class and Sub-class appropriate relief, including actual or statutory damages and multiple damages;

C. Enter judgment in favor of Plaintiff and the other members of the Class and Sub-class, and against Defendants under the legal theories alleged herein;

D. Award reasonable attorneys' fees, costs, and expenses;

E. Award and the other members of the Class and Sub-class pre-judgment and post-judgment interest at the maximum rate allowable by law;

F. Award Plaintiff and the other members of the Class and Sub-class equitable, injunctive and declaratory relief as may be appropriate under applicable laws. Plaintiff on behalf of the other members of the Class and Sub-class seek appropriate injunctive relief designed to ensure against the recurrence of a data breach by adopting and implementing reasonable data security practices to safeguard Ubers' riders' and drivers' personal information, by an Order requiring Uber to implement reasonable data security enhancements as they become available, including data encryption, segregation of sensitive data, more robust passwords, authentication of users, increased control of access to sensitive information on the network, and prohibitions of mass exports of sensitive data;

G. Enter Declaratory Judgment in the form of a declaration that (a) Uber's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in

order to comply with its contractual obligations and duties of care, Uber must implement and maintain reasonable security measures;

H. Enter such additional orders or judgment as may be necessary to prevent a recurrence of the Breach and to restore any interest or any money or property which may have been acquired by means of violations set forth in this Complaint; and

I. Grant such other and further relief as the Court deems just and proper.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: March 22, 2018

By: *s/ Patrice L. Bishop*

Patrice L. Bishop
STULL, STULL & BRODY
9430 West Olympic Blvd., Suite 400
Beverly Hills, CA 90212
Tel: (310) 209-2468
Fax: (310) 209-2087
Email: service@ssbla.com

Howard Longman
Melissa Emert
STULL, STULL & BRODY
6 East 45th Street
New York, NY 10017
Tel: (212) 687-7230
Fax: (212) 490-2022
Email: hlongman@ssbny.com
memert@ssbny.com

David Pastor
PASTOR LAW OFFICE LLP
63 Atlantic Avenue, 3d Floor
Boston, MA 02110
Tel: (617) 742-9700
Fax: (617) 742-9701
Email: dpastor@pastorlawoffice.com

Counsel for Plaintiff